Turvaintsidendid

Peeter Tatter

peeter.tatter@kkp.pol.ee

Teemade jaotus

- Intsidentide halduse korraldamine
  Info- ja küberturbe korraldus - 06.11.2008, 1,5h
- Intsidentide haldus, taktika ja praktika
  Infosüsteemide ründed ja kaitse - 22.11.2008, 3,0h
- Arvutikriminalistika (computer forensics)
  Kurivara, 20.11.2008, 3,0h

Turvaintsidendid

Teatud vaatenurgast lähtudes on kogu andmeturbes käsitletav probleemistik taandatav kaheks suureks teemaks:

- intsidentide vältimine
- juhtunud intsidentide korrektne käsitlemine

Mis iseloomustab turvalist infosüsteemi?
Kuidas mahuvad siia turvaintsidendid?

Turvaintsidendid

- “Ennustamine”
- Valmistumine
- Ootamine
- Reageerimine
- Lahendamine
- Analüüs
- Turvapoliitika täiendamine

Turvaintsidentide ettenägemine

- Absoluutne vältimine pole võimalik
- Võimalike riskide teadvustamine
- More security doesn't make you more secure, **better management does** – mitte ainult vahendid ja meetmed, kindlasti ka personal ja protseduurid

Intsidentideks valmistumine

Planeerimine, dokumentatsioon

- ohuhinnangud
- tegutsemiskavad (taasteplaanid)
  - mida teha
  - kes teeb
  - kuidas teeb
  - talletab ja jagab infot tehtu kohta

Intsidentideks valmistumine

Meetmed

- monitooring - intsidendi avastamine
- logimine - info juba toimunu kohta
- valmisoleku testid

Optimaalsete meetmete leidmine 1

maksimaalprogramm:

- 24/7/365 online monitooring
- 100% logimine

Praktika:

- vajalik info kaob mitteolulise sisse
- kaob monitoorijate terasus
- IT-l saab kõrini logide mahutamisest

Optimaalsete meetmete leidmine 2

minimaalprogramm:

- “monitooringuks on kasutajad või kliendid, kui midagi on valesti, siis helistagu kasutajatoele, sealt tehakse häiret”
- “pole mõtet ette põdeda, kui midagi juhtub, siis lahendame asjad töö käigus”

Praktika:

- tõsised probleemid avastatakse liiga hilja
- puudulik ülevaade toimunust

Optimaalsete meetmete leidmine 3

mida meetmete valikul silmas pidada:

- uppuja päästmine on eelkõige uppuja enda asi
- olematut infot ei saa osta ka kalli raha eest (raha on võimalik ära kulutada küll)
- halbadel asjadel on paha komme korduda
- ressursse on alati piiratult – olemasoleva kasutamist tuleks hoolega planeerida

Töö käigus kohatud probleemid 1

Puudulik “paberimajandus”:

- kasutajad, kellele pole tutvustatud nende õigusi ega kohustusi
- administraatorid, kelle töö kohta puuduvad reeglid ja järelevalve
- süsteemid, mis on jumalast

  ehk asi loodi kunagi aegade alguses ning keegi ei tea täpselt selles toimuvat – siiamaani on töötanud

Töö käigus kohatud probleemid 2

- Firmad kes ei tea, mis info nende valduses on ja mis selle tegelik väärtus on
- Turvapoliitika on olemas ja kinnitatud, kuid praktikas seda ei järgita
- Probleemid vastutuse jagamisel, üks struktuuriüksus tegeleb infosüsteemi ühe osaga, teine teisega